European Journal of Law and Technology, Vol 11, Issue 1, 2020

EJLT European Journal of Law and Technology

3D Printing and the Right to Privacy: Proposals for a Regulatory Framework

Dr. Annika Jones * and Dr. James GH Griffin **

Abstract

Digital watermarks placed within 3D prints pose a challenge to the privacy of individuals. These watermarks are ubiquitous to every single 3D print, and thus can be used to track and trace the use of that print. The tracking can be achieved through any Internet connected device capable of detecting a watermark, such as a camera on a laptop or mobile phone. The unique nature of each watermark means that the use of an object by an individual is easier to trace. The ubiquity of watermarks in 3D printing poses a challenge to the privacy of the individual. This paper proposes three recommendations to deal with this challenge. Firstly, that the potential for digital watermarks to invade privacy should be addressed in relevant copyright treaties and under the international human rights law framework, secondly, that a voluntary code of conduct be established that supports the promotion of privacy through self-regulation of watermarking and 3D printing, and thirdly, that there should be a regulatory body to provide guidance and oversight.

1. Introduction

Developments in 3D printing have prompted commercial growth and social progress in a wide range of sectors, from the medical profession to food and farming. Nonetheless, due to combined developments in tracking and watermarking technologies, 3D printing poses a grave and growing threat to the privacy of individuals. While much has been written on the implications of technological developments for the right to privacy, little research has been undertaken into the specific privacy challenges that are being raised by innovation in 3D printing technology and the measures that can be taken to support more robust protection.

This article fills the gap by identifying the implications of developments in 3D printing for the right to privacy and proposing a technological framework through which they could be addressed. The research draws from a series of 30 in-depth interviews carried out with representatives of Chinese 3D printing companies over a 12-month period in 2016. [1] China was chosen as the focal point for the research because of the high level of innovation that is being driven by Chinese 3D printing companies, which provides an indication of where the technology is developing and where privacy issues are being raised. While China is used as a case study, the aim of the research was to draw broader conclusions about the adequacy of

privacy protection under international law in light of the most recent technological developments in this field. These conclusions are particularly significant in light of ongoing efforts in the field of international human rights law to identify ways of protecting privacy amid the rise of big data and associated technological developments. [2]

Drawing from the empirical research, the article puts forward three recommendations to enhance protection of the right to privacy in the context of developments in the 3D printing industry: (i) that recognition of the potential for digital watermarks to invade privacy is recognised in relevant treaties on copyright law and under the international human rights law framework; (ii) that a code of conduct is established that promotes privacy through self-regulation of watermarking and 3D printing, and (iii) that a regulatory body is established to provide guidance and oversight.

The article is divided into four parts. Section 2 highlights recent technological developments in 3D printing that raise privacy concerns, looking in particular at the significance of the nexus between 3D printing and watermarking and tracking technology. Section 3 outlines developments in the legal protection of privacy amid the rise of big data and related technological developments, including developments in international copyright law and international human rights law. Section 4 presents the results of the empirical research, which highlights the current stage of development of the relevant technology and privacy issues that are being raised in practice. Section 5 puts forward recommendations for more robust protection for the right to privacy in the context of 3D printing. Section 6 shows how the recommendations might be implemented, working with two case studies.

2. 3D Printing and its Implications for Privacy

3D printing will have a profound impact upon our notions of social privacy, and in particular notions of privacy within the law. While there has been a realisation of the privacy implications of the 'Internet of things' [3] - the rise of interconnected devices - there has been no attention paid to 3D printing and privacy issues. This is significant because 3D printing has the potential to be considerably more invasive than the Internet of things. 3D printed products can contain tracking technologies, not just within the computer files but also within the physical products themselves. Every physical product that is 3D printed has the potential to be tracked in a way that has never occurred before. In the future, as 3D printing becomes more common place, everything in the world has the potential to be traced, tracked and observed, which can reveal an incredible amount of information about the users of such content. This creates much opportunity, e.g. in the collection of information about product use that can be used to reduce product costs and to allow for the creation of products more closely tied to the needs of a consumer, but it also poses a direct challenge to the privacy of individuals. It also provides a challenge to the nature of legal regulation, as the underlying technologies are precise in application compared to the generalised principles of law.

The potential for tracking is even greater when considering the application of 3D printing within certain industries combined with future technological developments. For instance, with biotech printing there is potential for all 3D printed enhancements or bio printed materials to be traced. This can mean that someone with 3D printed blood vessels, for instance, could be traced, having their blood signs monitored all of the time in a way that people with purely natural blood vessels might not be able to be traced. [4] Such users may have limited control over what is being obtained in terms of information. [5] In terms of future technologies, the tracking of

content that is 3D printed also poses a challenge to privacy because of the ways in which it interfaces with these other technologies. The rise of artificial intelligence is likely to mean that a limited amount of tracking will be used to anticipate future actions, and uses of products, by users. This will be allied to the rise in big data in order to provide accurate data sets about predicated future uses.

There are also other developments such as 4D printing, which is where materials print themselves. In the future this could end up in the scenario where objects that are printed or material printed within the body is suddenly changed in shape or form and is able to reveal things about the actions of the user. [6] In addition, other technologies such as augmented reality and virtual reality are likely to interface with 3D printed content, again meaning that there is a lot of interchange data between the 3D printed product and the virtual forms of that product, allowing for the possibility of enhanced tracking. [7] All developments with regard to privacy and 3D printing have been highly dependent upon the development of associated and linked technologies. This is not an area which can be placed within an isolated context; indeed, this is an area which is likely to become increasingly mainstream and commonplace and so it is necessary to be aware that due to the convergence tendencies of digital technology [8] it is likely that 3D printing will incorporate elements from these other technical fields. Any proposed regulation of the right to privacy should take into account these potentially invasive characteristics, and take into account the increasing precision of such technologies compared to the often generalised nature of international law.

Much has been written about 3D printing and this paper does not seek in any way to replicate what has been written before. [9] However there has been far less attention paid to the tracking technologies that underlie 3D printing and it is this that the paper seeks to explain in terms of operation in order to explain their privacy implications.

The development of watermarking technology is largely a convergence of existing areas of technology. Firstly, there is technology that has existed in relation to simply identifying content. An example of this is the digital object identifier for digital content, and its earlier form, the ISBN barcode number that is found on many everyday objects. [10] There is also the use of technologies such as QR codes, which are a form of barcode that can reveal the distribution chain of a product. [11] These are technologies that enable the tracing of products that users 'want' to be traced. However, it is also necessary to consider technologies that are used to trace content that people do not want to have traced. These are the technologies used by States for surveillance purposes and technologies used by computer coders to be able to break into computer systems. [12] These technologies will play a very important role in terms of future content tracking. This is because these technologies are largely designed to predict what people might do based upon their previous actions. This is of value to companies such as movie studios who want to know what sort of content people have been watching in order to know how to invest in new content in the future. [13] The more information that they have the more accurately they are able to identify the habits of users. This is something that is likely to become increasingly important in as more content is being made in a tailored fashion, [14] and in a way that perhaps will require less expenditure. These technologies are central to both watermarking and State surveillance, thus it is necessary to bear in mind the issue of state surveillance when considering how surveillance technologies placed into watermarked 3D printed objects.

The technologies of surveillance have been around for a long time [15] - they are built into the very backbone of the Internet. Although it has been commonly said that the Internet protects the identities of individuals - as the The New Yorker famously once said "On the Internet, nobody

knows that you are a dog" [16] - the reality is that IP addresses are always identifiable. [17] Whilst Internet addresses are temporarily assigned in through TCP/IP protocol, [18] these can be actively monitored, as in the case in China. [19] It is this sort of technology, where users are identified for the purposes of records, that 3D printing watermarking technologies come into their own.

So, the technologies that need to be assessed are those that deal specifically with watermarking, and those that deal with state surveillance. With regard to watermarking technology, the traditional approach was to provide technology that was more passive in nature. For example, an ISBN number would provide information about the name of an author or publisher. [20] QR codes reveal the distribution chain of the product. [21] A DOI number provides information about a permanent Internet address for a piece of Internet content. [22] This passive information has recently been protected by what is known as digital rights management law. While digital rights management law is mainly known for its regulation of DRM mechanisms that control access and unauthorised reproduction to copyright works, there are complimentary provisions that protect 'RMI', or rights management information. RMI is just simply a way to identify content that is used to assess the levels of access or reproduction that is to be debated over certain content. It sounds innocuous, but the provisions protect information that can be in the form of digital code. There is discussion about applying this form of fingerprinting technology into the file format for 3D printers. Discussion has primarily focused around the STL file format, and adding in a form of encryption upon it into which metadata (which could enable licensing) can be added. This is the file format of PDF3D. [23] One of the issues with the existing STL file format is that it is very much a barebones format, in the sense that they contain state of X, Y and Z axes rather than any other information. [24] This means that any licensing systems of the sort proposed by the Copyright Hub are reliant upon outside information about the status of a particular file, which makes the system more prone to abuse. However, whichever direction the STL file format takes it should be noted that the development of surveillance technologies means that this deficiency of the STL file format is likely to become less important as the years progress. The advantage of having a file format that contains licensing information, the potential for watermark within the file, is that it reduces the need for more general surveillance technologies to be able to assess whether a file is being used in a manner that has not been licensed.

Surveillance technologies are not new, but the specific application of these technologies within the digital sphere has been particularly erosive of privacy of the individual. The revelations of Edward Snowden, Chelsea Manning and Julian Assange have revealed systems of mass surveillance being run by states, to the extent that recordings were being kept of every single individual's phone calls, emails and web browsing history. [25] The systems, such as the US PRISM system, were lacking sufficient legislative and executive scrutiny. [26] Mass surveillance such as this is necessarily dependent upon software that can filter the large amount content, for instance, to be able to assess who is a potential terrorist threat. This technology is essentially seeking to track the actions of individuals, which is something that is particularly useful in the commercial sector, and indeed is the sort of technology that is used by companies such as Spotify and Netflix, and underlies the principles of web 3.0.

The success of this form of surveillance is reliant on access to "big data". [27] Mass collection of data enables the computer software to be able to analyse and assess the future actions of individuals more accurately. With regard to 3D printing, it has already been noted in our empirical interviews that some 3D printers monitor the actions of individuals. [28] It is a small step to seeing this could be applied to the online licensing of 3D printed content, partly because

it helps companies to be able to more appropriately invest money in the future, but also because it is a means by which to be able to assess whether users are committing copyright infringement. With the rise of the Internet of things, and the increasing complexity of watermarking technologies that can survive transfer between different file formats (i.e. from the 3D printed product through to a photograph), the tracking of 3D printed content by methods similar to that used in tracking big data and the state surveillance of individuals becomes increasingly apparent. All it requires is a simple transposition of one set of technologies from one area (i.e. state surveillance) to that of the surveillance of 3D printed articles.

3. The Legal Framework for the Protection of Personal Data

The following sections look at the protection of personal data at the international level under two key frameworks - international copyright law and international human rights law - and highlight their limitations in providing protection for the right to privacy. The growth in 3D printing technologies and the threats to privacy referred to above are the result of specific actions by certain coders and re-users, with that underlying technology being precise and specific in its application. Reforms are therefore proposed in sections 5 and 6, which provide both generalised principles and specific code solutions to the privacy issues posed by 3D printing.

3.1 DEVELOPMENTS UNDER INTERNATIONAL COPYRIGHT LAW

Protection of personal data is addressed under international copyright law at the international, regional and domestic levels. The World Intellectual Property Organisation ('WIPO') Copyright Treaty of 1996 governs rights management information at the international level. [29] This treaty has been implemented globally within member states; [30] notable countries not to implement it are Iran and China. [31] The impact of the provisions has been twofold. Firstly, protection over such information encourages the collection of it. Secondly, the requirement of knowledge means that to safely protect that information there is a need to also employ technical means. In any event, such information might very well have been necessary for the operation of the majority of digital rights management mechanisms, and so one may argue that it is inevitable that this sort of data would be collected by companies. The impact upon privacy, though, is such that whilst the data is collected, there is no corresponding provision that exists in terms of how the collected data may be used.

Developments along these lines have been seen in UK case law under the common law of the tort of misuse of private information. There is, however, much uncertainty in this right, especially in terms of whether it is free standing [32] or based within the law of confidence. [33] This has implications in terms of the rigidity of the test used, and possible remedies for any invasion of privacy. If based in confidence, the test broadly is whether information is of the right type, that there be an obligation of confidence, and that there be an unauthorised use of the information to the communicators detriment. [34] In 2005, Vidal-Hall v Google [35] (heard in the Court of Appeal) allowed a claim against the collection of Internet browsing information that was performed without the consent of the user, Sharp LJ MR stating that "..we cannot find any satisfactory or principled answer to the question why misuse of private information should not be categorised as a tort for the purposes of service out of the

jurisdiction. Misuse of private information is a civil wrong without any equitable characteristics". [36] There is a clear analogy to be drawn between tracking Internet use and tracking the use of 3D printed objects. Nonetheless, the inherent uncertainty of the tort, coupled with its national jurisdictional nature, limits its applicability. This means that the privacy of user data is less likely to be protected than if the tort were more certain.

In addition to this limit to the protection of user privacy, user information could be revealed where a right holder seeks to obtain the identity of a user, for example, in the instance of copyright infringement. This can be done under the Norwich Pharmacal order, [37] as used in Golden Eye v Ben Dover Productions. [38] This could be used in situations in which a user may not want to reveal their identify - e.g. as with the sort of pornography in the Golden Eye case. Nonetheless, there are no safeguards other than basic ones mentioned in Golden Eye, namely the need to specify particular (and not random) fines for infringements, to clarify that the determination is not a final finding of infringement and that an appeal is possible. [39] Privacy is not a factor, and thus, again, user information from watermarks concerning the use of 3D printed content will receive very limited protection. Following the Telefonica case, [40] it is up to individual Member States to strike a balance between privacy and property rights. [41] That case was about revealing individual identities of Kazaa users, and concerned the issue of copyright infringement. The CJEU missed an opportunity to rule on how to balance competing rights of privacy and freedom of expression under the EU Charter; and so the protection of individual user privacy with regard to watermarked 3D printed content remains extremely limited.

A lack of international regulatory direction has left the development of tracking watermarking technologies unhindered. Indeed, there has even been some encouragement of this sort of tracing watermark technology within United States case law. The seminal case, which has been somewhat overlooked, is that of Grokster - not the well-known Supreme Court case of 2005, [42] but the one heard within the Central District of California in 2007. [43] This case, which was heard by District Judge Wilson, favoured the implementation of what was termed fingerprinting technology to establish which users may or may not be infringing copyright content. This is the first time that the use of active technology to enable tracking, as opposed to simply blocking content, was supported by a court. In the words of District Judge Wilson:

"Based on the Ninth Circuit's Napster decisions, products capable of substantial noninfringing use can be filtered if the failure to do so would constitute either continued contributory infringement (in the form of material contribution) or vicarious infringement. It would therefore be anomalous if such filtering were always unavailable where a defendant has only been held liable for inducement." [44]

The reliance on the rehearing of the enforcement of the Napster decision [45] should not downplay the importance of the judgment, since at the time the Napster judgment was heard the filtering technologies were not of the same magnitude (or effectiveness) as at the time of the Grokster judgment. [46] Indeed, as was noted in Napster, "The district court was dissatisfied with Napster's compliance despite installation of a new filtering mechanism. The new filter analysed the contents of a file using audio fingerprinting technology and was not vulnerable to textual variations in file names." [47] Nonetheless, this does not excuse the lack of consideration of privacy concerns. [48] A similar situation has arisen in the CJEU with the cases of Netlog and Scarlet, which in effect have favoured an approach which can allow for ISPs to enact a filtering mechanism for the purposes of copyright enforcement. This is so provided that they are not for

an unlimited time, exclusively at the expense of the ISP, if it is merely preventative, applies indiscriminately to all users, or for information stored on the servers by service users. [49]

More recently, there have been moves by the EU executives and legislatures to require filtering technologies. Again, they have not taken account of privacy concerns. The original EU Digital Single Market Directive on Copyright [50] contained Article 13 (now 17) which stated:

"Information society service providers that store and provide to the public access to large amounts of works or other subject-matter uploaded by their users shall, in cooperation with rightholders, take measures to ensure the functioning of agreements concluded with rightholders ... such as the use of effective content recognition technologies, shall be appropriate and proportionate." [51]

The final version that has become law does not refer to those recognition technologies, [52] but the requirement to have licensing remains - and such recognition technology is critical to ensure that. Clearly, such measures pose privacy concerns but there is nothing in the Directive that directly deals with that issue. Thus far, the more generalised regulation concerning big data of personal information has also been ineffective, especially in the context of mass surveillance.

Another issue regarding the current regulation of 3D printing concerns data protection. 3D printing raises unique issues for data protection because of the difficulty in relying on consent for the use of personal data in this context. This is because a digital watermark can be used to construct data about the use of an object, but a user may not have consented to (or even been aware of) the watermark. Information is not collated directly from the user as such, but from the object. The object data can then be stored and observed subsequently, in the same way as a Google search is carried out in relation to websites. This makes the legal regulation of data protection problematic. It may be extremely difficult to trace original users when content is going to be used in a new or novel way; furthermore, that information could be harvested without users consent from publicly available datasets of watermarks, used in a way not considered at the time. Given the global nature of the Internet, it is not unreasonable to consider that such information find its way online, perhaps with the consent of the user but for other purposes; third parties could then find new ways to utilise the data. Those third parties may also be outside of jurisdiction. Nonetheless, the EU General Data Protection Regulation (GDPR) [53], in the absence of an alternative legitimate basis for data processing [54] requires explicit consent to be obtained for the collection of personal data, the practical application of consent can be limited. [55] In China, a similar regulatory situation arises, with the Cybersecurity Law of 2017. [56] This also requires the consent of an individual when collecting data about that person. [57] Again, in practice, subsequent re-use of data in unexpected ways could lead to that consent being largely meaningless.

To reiterate, the specific issue that consent raises is that consent can become simply irrelevant due to the way the data about use is collected. Firstly - and self-evidently - a watermark is a means by which to locate an object. The data itself does not identify the user - it is the combination of the watermark with other publicly available data that poses the danger to privacy. In this sense, the challenges may appear like those that arise with photographs. A photograph might be used in a search for anything, for instance with the use of Google images. However, whilst the taking of a photograph may require consent when that photograph is taken of an individual, the same is not true of photographs as objects per se . A watermark merely makes it easier to discover an object (or photograph). It would still be discoverable through image recognition, but it might take longer. With the development of AI there will be an

increased ability for computers to quickly identify objects, and watermarks will therefore become more important in terms of identifying the sources of printed goods.

Watermarking therefore poses a challenge to the applicability of consent in relation to generalised data protection laws. It is necessary to look to broader principles of privacy under the international human rights law framework, in order to provide an adequate regulatory regime for privacy concerns.

3.2 DEVELOPMENTS UNDER THE INTERNATIONAL HUMAN RIGHTS LAW FRAMEWORK

International human rights law provides a useful framework for dealing with privacy issues because of its universal nature and, consequently, its ability to address issues that cross borders, such as digital information flow and aspects of the 3D printing industry. In response to technological developments and the rise of big data, questions have been raised about how the right to privacy should be interpreted and attention has been drawn to the limits of informed consent in the protection of personal data. These issues, however, remain unresolved. It is the purpose of the recommendations below to show how the right to privacy can be protected in the context of developments in 3D printing.

The right to privacy has been incorporated into a wide array of international and regional human rights instruments, [58] in addition to legislation at the domestic level. These measures operate alongside regional measures that have been taken specifically to enhance the protection of data privacy, such as the EU GDPR. [59] At the heart of the international framework lies Article 12 of the Universal Declaration of Human Rights, [60] which provided a basis for the development of an enforceable international treaty obligation under Article 17 of the International Covenant on Civil and Political Rights (1977) (ICCPR). Article 17 ICCPR requires that "[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation" and that "everyone has the right to the protection of the law against such interference or attacks". [61] Article 17 enshrines a limited right, which is confined to interference with privacy that can be deemed "arbitrary or unlawful".

Whilst the international human rights framework is in many respects well placed to address the privacy issues that have been raised by 3D printing, it has two notable limitations. The first is the lack of universal ratification of key human rights treaties, including the ICCPR. China, for example, is a non-State party. The second is the lack of clarity as to what is, and should be, encompassed by the right to privacy in an age of developing technology and the rise of big data. The articulation of the right to privacy in Article 17 is broad and provides little guidance as to how specific concerns raised by 3D printing, big data and other technological advances should be addressed. Only limited guidance can be drawn from General Comment Number 16, produced by the ICCPR's monitoring body, the Human Rights Committee (HRC) in 1988. [62]

Prompted by concern about the use of "big data" in the context of State surveillance, the General Assembly produced Resolution 68/167 on "The Right to Privacy in a Digital Age" in 2013. [63] The Resolution has been deemed significant in, amongst other things, starting a "conversation" on the relationship between human rights norms and data collection activities and by addressing the issue of surveillance, interception and data collection "in human rights terms". [64]

General Assembly Resolution 68/167 supported the continuation of the discussion on human rights and new technologies by requesting the Office of the United Nations High Commissioner for Human Rights to produce a report on "the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or the interception of digital communications and the collection of personal data, including on a mass scale". [65] The report was finalised in 2014. [66] It recognised the conflict between the value of digital communication technologies, on the one hand, and their impact on the enjoyment of human rights, on the other. [67] Importantly, it rejected the idea that "individuals voluntarily surrender information about themselves and their relationships in return for digital access to goods, services and information" and raised questions about "the extent to which consumers are truly aware of what data they are sharing, how and with whom, and to what use they will be put". [68]

The report is significant in the context of this article because it recognised that the interception or collection of data about a communication - or "metadata" - could constitute an interference with privacy, given the insight that it might offer into "an individual's behaviour, social relationships, private preferences and identity", regardless of whether or not it is "subsequently consulted or used". [69] The use of such metadata is, as already discussed, a key concern that is raised by 3D printing and tracking technology. While the report focused on the issue of mass surveillance, it began to address questions about how the right to privacy should be conceptualised in a new digital environment, which are of broader significance, including in the context of commercial activity and 3D printing. It did not, however, address the specific issues that have been raised by the combination of 3D printing and tracking technology that have since emerged.

One of the important aspects of the OHCHR report, in the context of digital watermarking for 3D printing and the code of practice recommended below, is its emphasis on the role of business in protecting the right to privacy in the digital age. The report recognises the Guiding Principles of Business and Human Rights, which were endorsed by the Human Rights Council in 2011, as "a global standard for preventing and addressing adverse effects on human rights linked to business activity". The principles recognise that business enterprises have a responsibility to respect human rights. The responsibility to respect requires business enterprises to "tak[e] adequate measures for their prevention, mitigation and, where appropriate, remediation". [70] In order to do so, business enterprises must engage in human rights due diligence, a process which "should include assessing actual and potential human rights impacts, integrating and acting upon the findings, tracking responses, and communicating how impacts are addressed". [71] The OHCHR report recognises that the responsibility to respect "applies throughout a company's global operations regardless of where its users are located, and exists independently of whether the State meets its own human rights obligations". [72]

Applying the Guiding Principles to the communications and information technology sector, the report emphasised that Internet service providers and suppliers of digital communications technology and equipment "should adopt an explicit policy statement outlining their commitment to respect human rights throughout the company's activities" and "have in place appropriate due diligence policies to identify, assess, prevent and mitigate any adverse impact". [73] The voluntary code of conduct, proposed below, provides a means of working towards compliance with this obligation in the context of developments in 3D printing.

Following the adoption of the OHCHR report, and prompted by the General Assembly in Resolution 69/166, [74] the HRC adopted Resolution 28/16, appointing a Special Rapporteur on the Right to Privacy. The Special Rapporteur engaged in a process of establishing "a better

understanding of what privacy is, or should be, across cultures... in a way that is relevant to a digital age in which the Internet operates without borders". [75] Reporting to the Human Rights Council for the first time, in 2016, the Special Rapporteur spoke of challenges posed by the rise of private corporations "operating across national borders and attracting customers throughout the world", leading to an "increasingly detailed data map of consumer behaviour [that] has resulted in personal data becoming a commodity". [76] The report raised concerns similar to those mentioned in the report of the OHCHR concerning the awareness of consumers as to how the data that they generate through online interactions may be used, and their consent to its use. [77]

The Special Rapporteur outlined a 10 point action plan, which included areas such as work on the meaning of the "right to privacy", awareness raising and the "creation of a structured, ongoing dialogue about privacy". [78] Significantly, the action points included "[a] renewed emphasis on technical safeguards", acknowledging the need, beyond law, for "effective technical safeguards, including encryption, overlay software and various other technical solutions where privacy by design is genuinely put into practice". [79] This indicates receptiveness to the type of technical solutions that we propose in relation to 3D printing, below. The emphasis of the Special Rapporteur on technical standards takes place alongside consideration of the development of hard and soft law instruments, including an additional protocol to Article 17 of the ICCPR. [80]

Concerns about reliance on the impact of technological developments, including AI, on the right to privacy and the difficulties in relying on informed consent to the use of personal data are reiterated in subsequent reports of the Special Rapporteur [81] and the OHCHR, [82] and in recent resolutions of the Human Rights Committee [83] and UN General Assembly. [84] The reports and resolutions reaffirm the role of business enterprises, as well as States, in responding to privacy concerns and acknowledge the need for technical solutions to tackle privacy issues.

It is apparent from the above that continued effort is needed to understand what is needed to protect the right to privacy in light of technological developments within and beyond the 3D printing sector and the limitations of informed consent in this context. The international framework for the protection of the right to privacy is generalised and does not deal with the specificity of infringements potentially caused by watermarking in 3D printing. The technical solutions that we propose to respond to these issues are informed by our empirical research into developments in 3D printing, which are outlined in the section below.

4. 3D Printing and the Right to Privacy in Practice: Insights from Practice

Data drawn from interviews with 3D printing companies in China provides an insight into current developments in the technology and extent to which privacy concerns are being raised in practice. They also indicate a demand within the industry for more detailed guidance as to how personal data can and should be protected.

4.1. CURRENT USE OF PERSONAL DATA IN 3D PRINTING COMPANIES IN CHINA

While several participants stressed that they were not saving data or files from customers, [85] the interviews indicated that there was a widespread recognition within the industry of the value of the personal data that could be collected in the production and use of 3D printed materials.

The majority of the interview participants considered personal data to be valuable. [86] One participant considered the value of the personal data to differ depending on the sector concerned: tracking data would, he believed, be more useful in the medical sector than in the context of household objects. [87] The main use of personal data described in the interviews was in product development, [88] including medical devices". [89] When discussing the value of personal data, most participants remained focused on its use in the development of 3D printed products rather than its more general commercial value, [90] indicating that this is an area that has not yet been fully exploited in the way that it has been in other sectors (such as in the use of search engines and social media). Two interviewees did, however, recognise the value of "big data" produced elsewhere for use in the 3D printing industry. [91]

The interviews also revealed the sensitivity of some of the data that was being collected in the production and use of 3D printed products, particularly in the medical sector. One participant described how 3D printing was being used to demonstrate or simulate surgical operations. [92] A CT scan would be used to make a 3D printed replica of the relevant body part, which could then be used to plan the operation. [93] He gave the example of an operation on a brain tumour: "the brain will be scanned, when doctors cannot exactly make sure where it is, then we use 3D printers to print it out to find the best place for needle to go through the brain and get the tumour out". [94]

Another participant explained how personal data could be used in the design of medical devices:

"...what we do now is using [sic] the data, 3D data of patient, and then we try to design the next generation of medical devices. So as you can see here, we have all the data of the patient, and then we design the coding guide, and artificial hip and elbow to fit the patients internal size and shape, so we design the medical device just for that patient. That is more important part. So the next step we are going to do is to use our 3D printer to manufacture the medical device, or the reconstructed model of the patient". [95]

In both of the examples above, the scan data that is used to make the 3D printed model is clearly of great sensitivity and raises considerable risks to the privacy of the patient.

4.2. TECHNOLOGICAL DEVELOPMENTS WITH PRIVACY IMPLICATIONS

Many of the interview participants recognised the value of watermarking and tracking technology for the 3D printing industry, although the value was not acknowledged by all. [96]

One participant acknowledged the potential use of tracking technology as a means of assessing the quality of materials to be used in 3D printing. [97] The majority, however, saw its value to lie in tackling piracy or copyright issues. [98] Only two participants questioned the value of watermarking as a means of tackling piracy issues. [99] One considered regular updating of the product to be a more practical means of protecting against piracy than watermarking. [100] One

interviewee mentioned that he was in favour of putting a watermark on a printed product, which would indicate that their company had produced it. [101] He acknowledged that their clients would not allow this but considered that a hidden watermark may be acceptable for the client if it was not visible. [102] The discussion highlighted the potential for tracking to be used beyond the client's consent. Another participant, involved in the production of 3D printed medical products, explained that they would print the name of the patient and the brand onto printed products to help identify them. [103] A third said that they would consider using watermarking to enable a system of payment if others were to use a watermarked file. [104]

None of the interviewees mentioned the commercial value of data that could be used by combining 3D printing with watermarking and tracking technology, suggesting that this is yet to become a widespread industry in its own right.

The interviews suggested varied use of watermarking and tracking technology to date. Two participants noted the capacity of their company to engage in tracking. One, involved in 3D scanning, explained that "[a]ll the 3D data has a traceable [QR] code... it can be tracked from the beginning to the end". [105] Another said that their company had the ability to track who downloaded files and where they were downloaded. [106] Some indicated that they were considering the use of tracking technology, [107] while others recognised that other companies were currently tracking data. [108]

Some representatives highlighted practical obstacles to use of the technology, [109] one raising questions as to its "technical feasibility". [110] One representative highlighted the issue of the costs involved in tracking, which, they believed, was prohibitive for lower value products. [111] Another, who confirmed that their company was not currently tracking data, highlighted two obstacles: (i) that 3D printers in China are off line, preventing tracking, and (ii) that a lot of software in China is open source and that watermarks could be removed. [112] Another company explained that the equipment that they were using had a tracking function but it was not being used because the printers were not connected to the internet. [113]

The data suggests that watermarking and tracking technology is being used to a degree, but that it is not yet extensive. While there is widespread acknowledgement of its value, the value is seen to lie primarily in ownership and protection against piracy and copyright, rather than in the collection of personal data for commercial exploitation.

4.3. PRIVACY CONCERNS WITHIN THE INDUSTRY

When asked about the collection and use of personal data obtained through the production and use of 3D printed materials, a number of interviewees noted the moral implications that this would raise. The process of tracking the use of 3D printed products was described by one interviewee as an "infringement" of the privacy of the individual:

"If we insert a chip, then it may be an infringement to the clients. In other words, I am tracking your path. Tracking how the documents are being used is another kind of infringement. For example, your shoes being inserted a chip to record your exercise is another way to report your location. The manufacturer could know every consumer's location. So the consumer's privacy has been exposed". [114]

Another participant acknowledged the implications of using patient data to develop products and produce academic papers in the medical sector. [115] They highlighted the importance of

getting the permission of the patient and considered the anonymization of the data to be a possible solution. [116] The same participant discussed the possibility of putting patient information about how surgery went on a cloud and stressed that they had a high standard of protecting privacy and would ensure that the information is not leaked, whilst noting the risk of hacking. [117] The issues raised by the interview highlighted two key privacy concerns raised by 3D printing, namely consent to use personal information and the security of information that is stored digitally. These two issues are addressed in the recommendations below.

A more general concern was the impact that collection of data would have on customer confidence. One participant opposed the idea of selling data related to a customer on the basis that "it will harm not only the markets of our customers, but also ourselves". [118] They noted the value of the data, but stressed that "if service providers use the data somewhere else, such as customize based on the data and then produce new product, which is fundamentally from manufacture, then customer might feel that it is not moral and it do harm to their own patent". [119] The underlying concern was the implications to the patent rather than the customer's right to privacy. Another indicated that they were hesitant about tracking how 3D printed products were used because of the willingness of consumers to accept this practice. [120] Describing the possible impact on customer confidence, another participant gave the following example: "I am living in a house with windows. What if I live in a house built by glass? Will you still live there?". [121] The same participant went on to say that "everyone has [their] privacy, you cannot monitor your clients because they buy your products". [122] The data indicates a consciousness of the growing worldwide consumer concern for "privacy-friendly products and services", which has been noted by the Special Rapporteur, [123] as well as his conclusion that "privacy has become an important commercial consideration". [124]

4.4. DEMAND FOR FURTHER REGULATION

The Special Rapporteur placed significant weight on the role that market forces will play in encouraging the protection of the right to privacy. [125] However, market forces have yet to provide sufficient guidance as to what protections are required in order to safeguard individual right to privacy. Several of the interview participants mentioned the absence, or inadequacy, of current regulation of privacy issues in the context of 3D printing. [126] One indicated that they were unaware of any government or industry regulation on the use of personal data. [127] Another mentioned that there was no regulation so far. [128] A third, working in the medical sector, considered that more regulation on the use of patient data would be helpful, explaining that:

"there is no discussion before and now, for example patients' information, but we do have some collaborations with the hospitals that they want to have any files they sent to us to help us to provide the services, they want to keep those confidential. But we don't think there are clear rules in 3D printing although they have rules for the hospitals in a general sense". [129]

Consequently, while competition around privacy protection in the 3D printing industry may act as a form of soft regulation, [130] the interview data suggests that it is not providing clear enough guidance to companies as to how privacy should be protected.

In the absence of clear guidance, some interview participants indicated that they were self-regulating in order to ensure that privacy was protected. One participant, working in the medical sector, indicated that their company was going beyond the current regulation in order to provide greater protection for personal data. [131] A second explained that "[b]ecause the 3D

printing is quite new, but before any law comes out we are not going to put our information into the open platform". [132] It was anticipated in one interview that regulation in China is likely to follow developments in the US and Europe, [133] indicating that companies might be pre-empting regulation, finding standards from beyond China. [134]

However, the general reform proposals favoured by the companies could lead to the erosion of privacy. For example, making a patent system more efficient, [135] could undermine the privacy of individual user details. Digital watermarking could, in theory, be used to observe the use of 3D printed products, tracing the actions of individuals. Indeed, the possible erosion of privacy due to enforcement has been seen within the UK, where letters have been sent to Internet users accusing them of copyright infringements. In Golden Eye v *Ben Dover Productions* [136] individuals were sued for allegedly downloading pornographic content. The courts have issued guidelines as to when and where letters can be issued. The point, though, is that these guidelines could be met with trackable 3D printed watermarks, and yet it would be extending legal enforcement of IP to an area not yet covered, namely the tracking and tracing of physical objects and the use of those objects by an individual. In view of the desire by 3D printing companies to see strong IP enforcement of their works, the status quo in relation to privacy is likely to be in favour of a breach rather than the protection of privacy per se. Indeed, looking at the implementation of the Digital Economy Act 2017, [137] attempts of previous legislation such as Digital Economy Act 2010, [138] and attempts in other countries such as France with the HADOPI law, [139] generalised IP enforcement measures do not address the specific challenges posed by tracing technologies such as digital watermarking, particularly with regard to 3D printing.

The picture that emerges from the data is that privacy issues are already being raised and that the risk of further incursions into individual privacy are on the horizon with the development of new technology and growing awareness of the commercial value of the personal data that can be collected through the production and use of 3D printed products. At the same time, it is clear that there is a demand within the industry for further guidance as to how to ensure that personal data, and individual privacy, is protected as the industry evolves. Particular concerns have gone to consent to the collection and use of personal data and the problem of data security. The international human rights law provides a framework to address these issues. There is, however, an issue surrounding its implementation in the context of 3D printing, which will be addressed in the recommendations below.

5. Developing More Robust Protection for the Right to Privacy: Three Recommendations

In light of the outcomes of the empirical research, we propose three measures to protect privacy when digital watermarks are used in 3D printer files and 3D printed works:

a) The incorporation of reference to the right to privacy in relevant copyright treaties and recognition of the implications of watermarking under the international human rights law framework;

b) A code of conduct that promotes privacy through self-regulation of watermarking and 3D printing;

c) The creation of an advisory body to provide guidance and oversight.

5.1. THE INCORPORATION OF REFERENCE TO THE RIGHT TO PRIVACY IN RELEVANT COPYRIGHT TREATIES AND RECOGNITION OF THE IMPLICATIONS OF WATERMARKING UNDER THE INTERNATIONAL HUMAN RIGHTS LAW FRAMEWORK

An international provision should be created to deal with the specific issues relating to watermarking in 3D printed objects. This provision could be inserted alongside the copyright management information provisions contained within the two main WIPO IP treaties. Within the relevant article, we propose that the following should be added:

"Copyright Management Information should not be used to infringe an individual's privacy by being used to track individuals or the use of objects without an express statement by the copyright holder to that effect."

The purpose of this wording is not to outlaw the tracking of individuals through watermarking, because individuals may want to make use of the possibility in order to substitute for upfront payment for goods. For example, advertising of a product could provide income to the original copyright holder thus removing the need for the user of a product to purchase it in original form. The privacy concern arises where there is the tracking of individuals where the individual is not aware of the tracking and thus invading privacy. For example, a digital watermark could be used to track and trace the use of 3D printed content within the home environment, revealing information about the private lives of users, e.g. to the level of knowing which objects someone has in their house, where objects are placed in the home, how they are used and with what other watermarked objects. The greater use of cameras with the undoubted rise of augmented reality devices, alongside the Internet of Things, could see a considerable increase in the ability to trace objects. The proposed treaty provision would therefore deal with these scenarios where privacy is potentially infringed. [140]

One issue with the concept of privacy, as applied to watermarking, is that it could lead to a conflict with the protection of IP rights. If an IP infringement is discovered (e.g. two objects suddenly appear to have the same or almost the same watermark, with the ability to differentiate the original product through the addition of other secret marks or different manufacture techniques) then if the IP right cannot be enforced there could be a conflict with other international provisions. In particular, there could be conflict with Article 13 of the TRIPS agreement:

"Members shall confine limitations and exceptions to exclusive rights to certain special cases which do not conflict with a normal exploitation of the work and do not unreasonably prejudice the legitimate interests of the rights holder." [141]

Under our proposal, digital watermarks themselves will be protected as part of IPR. [142] If we are limiting the application of IPR in a manner that falls afoul of the three-step test, then proceedings could be brought under a dispute settlement procedure against a member state. [143] The three-step test clearly states that limitations and exceptions should be confined to certain special cases; that they do not conflict with the ordinary exploitation of the work; and do not unreasonably prejudice the legitimate interests of the rights holder. Despite the possibility of arguing a legitimate interest, the issue remains whether privacy is something that should be a

limit or exception which is a special case which conflicts with ordinary exploitation. The approach we suggest is that, as with freedom of expression and the right to privacy, there should be a balancing of the interests. [144] This should be construed so as not to fall afoul of the normal exploitation of an IP work, nor should it curtail the right to privacy. It would be up to courts to strike that balance, in the manner in which it has been in case law to date.

As has already been noted, mainland China is not currently a signatory to the WIPO Copyright Treaty. Nonetheless, implementing an identical provision within domestic law [145] would be a step towards the protection of privacy within watermarking. China itself has recently undergone changes to its own copyright laws, [146] subsequent to a long consultation period. It is proposed that any further changes to the copyright regime in China consider the privacy implications in watermarking in the same manner as proposed above.

Through the proposed provision, it will be possible for signatory states to have a basis through which to implement amendments to laws or new laws made in order to protect privacy. From our earlier considerations of law concerning privacy and 3D printing, the main issue appears to be a lack of realisation of the potential privacy issues involved. Our provision would raise awareness of the issues concerned, and provide a legal basis by which to tackle the privacy issues raised. For example, the UK or China may want to implement a law in order to meet the international requirement, or the EU may wish to amend article 17 of the Digital Single Market Copyright Directive. [147]

The need for a specific response to the threat posed by 3D printing and watermarking technology should also be acknowledged under the international human rights law framework. Here, the right to privacy is protected but without reference to the particular issues raised by technology addressed in this article. This could be remedied by an endorsement of the code of conduct outlined below by the Special Rapporteur on the Right to Privacy. The code of conduct would provide guidance, indicating how the right to privacy could be upheld in the context of the technological developments that have been outlined above.

5.2. A CODE OF CONDUCT THAT PROMOTES PRIVACY THROUGH SELF-REGULATION OF WATERMARKING AND 3D PRINTING

A voluntary code of conduct would encourage self-regulation of 3D printing and watermarking in a manner that supports the right to privacy and would respond to the specific regulatory challenges that privacy in 3D printing and tracking technology poses. It would show how the generalised principles of privacy protection outlined above could be realised in this context.

The concept of self-regulation was suggested by some of our interviewees. The ability to be able to self-regulate has obvious competitive benefits, in that the stakeholders involved can maintain a level of regulation that maintains consumer confidence in watermarked products for the minimum of costs. Aspects of the code could also be incorporated into domestic law to allow for enforcement at the domestic level. As already discussed, it could also be endorsed by the Special Rapporteur on the Right to Privacy as a means of protecting the right to privacy in this context.

The code would include the following elements:

5.2.1. A REQUIREMENT THAT WATERMARKS BE CLEARLY IDENTIFIED ON 3D FILES AND GOODS

A kitemark should be included on all products from a manufacturer, guaranteeing that any product that knowingly has a watermark on it is clearly identified. The practice of stating clearly on a 3D file or print that it contained a watermark would in theory help to bolster customer trust in the marketplace, responding to concerns already being raised in the industry. [148]

The establishment of a code requiring the copyright holders to state clearly what the watermark could be used for would provide additional protection. The choices of a copyright holder could be framed as follows:

a) A watermark will be used solely in order to trace the origin of the product

b) A watermark will be used to track and trace the use of the product.

c) A watermark will be used to enforce the intellectual property within the object.

The relevant code would be clearly identified on an object. It would help to provide certainty in a manner similar to that which has come from the use of statements on Creative Commons licences. [149] Copyright holders could request the proposed oversight body [150] to provide additional categories. In addition to privacy concerns, there is the risk that watermarks will be applied to goods over which there is no IP, thus opening the possibilities of a) extending the reach of an IP style element over non-copyright parts, and b) enabling people to claim an IP style protection of works that were not originally theirs. [151] This could be true of aggregation websites, which might overlay watermarks to direct subsequent users back to their own website rather than the originator of the work. To guard against this, such watermarks could be challenged before a regulatory body. Details of that body will be discussed below.

The kitemark would be required to be applied to an object so that a user knows that a 3D printed object has a watermark and that their private data may be collected. It would be a violation of the code of conduct not to include a kitemark on an object with a watermark. For example, if a Star Wars 3D file on a website was downloaded and then printed, there would be a requirement to identify via the kitemark that the watermark was placed into the file. If a watermark was applied to a 2D object (such as a Star Wars character from a film), which could be so if the 2D image was applied as a skin to a 3D file, then there would be a requirement to apply the kitemark if the person producing the 3D file knew, or should have known, about the existence of the watermark. [152] This proposal responds to concerns about consent that have been raised in the abstract under IP and international human rights law, and have been acknowledged in practice. [153]

5.2.2. A PRINCIPLE THAT MEASURES MUST BE TAKEN TO ENSURE THE PROTECTION OF INDIVIDUAL PRIVACY WHERE IDENTIFYING MARKS OR MODES OF IDENTIFICATION ARE USED WITHIN AN OBJECT OR CODE

The code would embrace the following principle:

"Where an identifying mark such as a watermark, or equivalent mode of identification, is attached to, or within, an object or code for that object, measures must be taken to ensure the protection of individual privacy".

This would mean that when a watermark is placed on an object, that there should be safeguards in place to protect the identification of the user of the content. This requirement could be complemented by the proposal below that there could be soft regulation, which would encourage the adoption of encryption of individually identifying information that may be associated with the watermark. [154] This would respond to the concern raised in the interviews about the security of digitally stored information. [155]

The reference to an "equivalent mode of identification" is included as a way of preventing creators from using unusual shapes combined with AI as a way of circumventing the provision. Digital watermarks can be placed into an overall shape of an object, so if sufficiently obfuscated it could lead to courts mistakenly thinking that the shape does not form part of the mark. This provision would prevent that circumvention being a means of avoiding privacy requirements.

In terms of application, the protection of privacy could be achieved by anonymising data collected, perhaps decentralising it within an encrypted peer to peer system. Alternatively, data could be kept in some form of secure blockchain. [156] As with the last provision, this is all dependent on the knowledge held by the provider of the file. This is important as code can be placed within the watermark itself, so it is possible for a watermark to collect data and the person applying the mark not to know about it. In the Star Wars example above, this would mean that if a mark is placed within a 3D printed object, the person distributing the object containing the mark would be under an obligation ensure protection of privacy in the collection and storing of the data. However, if the mark is collecting (or enabling collection of) information without the knowledge of the person applying and distributing it, then that person will not be held liable. Liability would apply to the originator of the mark (e.g. perhaps Lucasfilm). If the person would have been expected to know about the existence of the mark, then that person would be liable.

5.2.3. A SOFTWARE COMPONENT THAT CAN ISOLATE AND PROTECT PRIVATE INFORMATION COLLECTED FROM A WATERMARK

As part of the self-regulatory process, we propose that there should be a specific software component that can isolate and protect private information collected from a watermark. For example, if a 3D printed organ contains a watermark to be able to observe the continued quality of the print (to preserve the patient's life) then that information should be encrypted and only be accessible by somebody who has an authorised key. [157] This software component could be incorporated into a file format standard such as those organised by the ISO, [158] or a software file format specifically for watermarks.

This would provide the means to facilitate an automated licensing system, whereby the actions of individuals would not be so traceable by other users or by the originators of 3D prints. A block chain could be kept to trace the transactions made independently of the individual information about use. This would mean that there would be a central ledger related to the existence and use of the object, which would be encrypted, but which could be kept separate from the ultimate identification of the actual user. This would be very similar to the ledgers used in currencies such as bitcoin. [159]

The issue is whether self-regulation will provide a sufficient means for the protection of individual anonymity. We would suggest that, without oversight, it would not be sufficient. Information about the use of products is an obvious additional source of money for copyright holders, and this poses a conflict between the protection of privacy and profit. For instance, a

copyright holder could make substantial money from observing and tracing the use of 3D printed objects - this could be similar to advertising, or it could be through other methods such as monitoring the quality of 3D prints by observing the structure of the watermark. While one interviewee in our study acknowledged that the market would require a protection of privacy in order to maintain confidence in the market, [160] concern for market confidence may be overridden by profit incentives. Furthermore, difficult questions might arise as to what is required to protect the right to privacy in specific circumstances, such as where consumers wish to reveal information about use in exchange for discounted products. Such questions could be resolved by an independent regulatory body, designed to provide oversight and guidance.

5.3. THE CREATION OF A REGULATORY BODY TO PROVIDE OVERSIGHT AND GUIDANCE

One way to deal with the issues that will arise in relation to the above proposals would be to have soft administrative regulation from a body appointed to monitor or provide guidance. It would be possible to achieve this through a collective licensing organisation such as the UK Copyright Hub or National Copyright Administration of China (NCAC). [161] The UK Copyright Hub already has domestic technical codes for online licensing, and this would have the advantage that the rules would be able to interface directly with the computer code, thus providing a technical means to protect privacy specifically in relation to digital watermarking. Another alternative would be for a body such as the UK Intellectual Property Office to provide guidance, or the Copyright Tribunal, although it should be noted that the Copyright Hub is designed as a complementary regulatory body in the field of online licensing. The use of any of these bodies would essentially provide a co-regulatory environment, similar to those in operation in other fields such as telecommunications and media. Given the international nature of 3D printing, and given that there are so many similarities between the concerns of companies in China to those in the West, a soft approach could make for easier regulation of common concerns. Another approach would be for the existing UK based Information Commissioners Office ('ICO') [162] to take on an extra role. That Office investigates breaches of the UK Data Protection Act 2018, and EU GDPR. The information commissioner has the power to levy fines in relation to data protection, [163] and so it might be possible to assign similar powers to the ICO to monitor and provide guidance. It might also be possible to refer to examples from the medical sphere regarding privacy of private information, although we submit that the different factual situation makes application difficult. [164]

The regulatory body would provide guidance on the application of the code of conduct. The enforcement of the voluntary code would operate alongside and in parallel to the enforcement of hard law treaty obligations found under the international human rights law framework, and under copyright treaties if the proposal outlined in Section 5.1 to add a privacy obligation to such treaties is adopted. The existing ADR structure for enforcement of the copyright treaties could be used to enforce the new obligation. [165] Signatory states (or individuals) [166] can bring actions for a breach of that provision, so, for example, if China believed the US had breached the privacy standards, it could bring an action. Compliance with the right to privacy under the international human rights law framework would continue to be addressed by its existing enforcement and compliance mechanisms, including regional and domestic courts, treaty bodies (such as the Human Rights Committee) and Universal Periodic Review by the Human Rights Council.

Enforcement of the proposed code of conduct (5.2.1-5.2.3) would be achieved through a separate administrative body via approved mediation routes. This would provide a means by which individuals or companies could challenge either signatory States or individuals who have not complied with its provisions, and where advice on compliance could be sought. Reporting obligations could be introduced to allow States and private companies who have signed up to the code of conduct to demonstrate their compliance with it, raise questions and benefit from feedback on their report. Any legal person, including non-signatories, could bring an action against a signatory of the code claiming non-compliance. So, for example, if an individual discovers that there has been a watermark placed within a 3D printed object, and that the watermark has been used to identify that individual without consent, the administrative body could make a finding that the code had been breached, which would then be subject to appeal.

6. Case Studies: Use of Watermarking in Specific Circumstances

To summarise, we have proposed i) a statement of privacy in relevant copyright treaties and recognition of the specific issue of watermarking in recommendations of the Special Rapporteur on the right to privacy, ii) a code of conduct that promotes privacy through self-regulation of watermarking and 3D printing, and iii) a body to give advice and regulatory oversight. During our interviews, two particular scenarios presented themselves where copyright holders could foresee a use for the watermarks. We will now proceed through these in order to establish how the proposals would operate in practice.

6.1. TRACKING AND TRACING ORIGINAL MATERIALS

One of the uses of watermarks favoured by the companies interviewed was regarding the source and quality of original print materials. [167] For example, one of the issues identified by an interviewee with biomedical 3D printing was over origin of the source material. [168] Currently there is no international standard to guarantee the quality of those materials, other than in relation to the most invasive medical uses, which in China are governed by certain requirements set out by the relevant regulatory medical authority. In terms of privacy, if that watermark is deeply embedded within the material to the degree that it could survive the actual printing process, it would provide a means by which the entirety of a product, from the creation of it through to the destruction of it, could be traced. This could pose privacy challenges in terms of revealing the use of products by individuals and companies without their specific consent. For example, someone with a scanner could detect which people have implants, or if they have 3D printed organ or 3D printed blood vessels.

Our proposal would require that a copyright holder state clearly on the material (or in the material in scannable form) how the information from the watermark could be used. Due to the (likely) confidential nature of the information, the confidential aspect could also be required under (e.g.) ISO guidelines to be encrypted. The code of conduct that we have proposed would require that the watermark is encrypted so that personal information would only be accessible if an authorised body has the decryption key.

A practical example would be if a hospital requires the printing of a titanium implant, say to replace a bone in a limb. Empirical data from our interviews shows that it is currently onerous to get regulatory approval for such an implant due to difficulties not just in the printing

technology, but also in guaranteeing the quality of the source material. A digital watermark could be placed within the original material to help guarantee quality, and also to ensure that the quality of the material remains undiminished after it is placed into the human body. The hospital, and patient, would be fully aware of any tracking potential as the producer of the material would be required to state this under our proposal. The identifying information about the individual would be encrypted within the implant, to protect against unexpected tracking, in line with our third proposal.

6.2. INFORMATION ABOUT THE USE OF A PRODUCT AFTER BEING PRINTED OR OBTAINED

Whilst some companies we interviewed had only limited interest in the utilisation of watermarking to monitor use, some had a specific interest, such as those in the biotech sector to be able to monitor the degradation of a 3D print when inserted into the human body. [169] Under our proposed system, copyright holders would be required to clearly state how a watermark will be used. This would mean that those applying the mark, be that the material producer or the printer of the product, would need to disclose the existence of the watermark to the final consumer, which ultimately would be the patient. That information could be kept confidential under the proposed self-regulatory framework.

However, in practice, it should be noted that tracking of use might be regulated through other incidental means. For example, whilst Internet searches using well known search engines will often suffice to identify the use of watermarked content, software might be required to track the watermark in more detail. Software may also be required for more complex watermarks and more complex information gathering. In the current example, this could mean that software could search for the signs of watermarked content, in order to then track the product use without permission. However, encryption of detailed individually identifying content should be able to remain confidential - it should only be the existence of the watermark that can be determined. One of the issues raised by the interviewees is that tracking of users could get out of hand, leading consumers to move away from 3D printing. [170] This is another reason why the code of conduct that we have proposed could prove popular. It would help to reassure the public that they will not be unknowingly watched by products.

By way of example, imagine that a user has printed out a drinking cup from the Internet on their own 3D printer. This cup has been used regularly for the past year. The user has drunk beer from it, and milk. The user lives in a house, where there are other connected devices, and the user uses a smart phone and wears Google Glass. The user has taken photographs of the house and placed these on Facebook and elsewhere on the Internet. Using the digital watermark information, it would be possible to Google search for photographs of the 3D printed mug. It would also be possible to for devices such as Google glass to record when the mark is within range. Over time, a geolocation pattern could develop about the usage of the product. The photographs could be analysed so as to detect the types of drink, especially if there is a watermark behind the drink, providing an additional point of reference. Advertisers could then take this information and target it against the user. Furthermore, if the cup is reproduced without permission, a copyright holder would then be able to trace the unauthorised copy, e.g. if our user had a friend scan the cup and reprint it at the friend's home, then this would be trackable - and for any subsequent copies. Our proposal would require that any mark being used for these purposes should state so clearly on the product itself. Furthermore, if there are infringement proceedings being brought against the friend (or against the user; regardless of the

law, the user might be pursued under the assumption the copy was made at the users own home) [171] then the international principles will require a balancing of the interests of privacy with the interests of legitimate expectation to protect the work under Art 13 TRIPS. If the voluntary technical code were being followed, then individually identifying information should not be available to third parties unless the user specifically enables such tracking.

7. Conclusion

The issue of 3D printing and privacy has long been overlooked. The field poses challenges far beyond that of the regulation of 3D printing per se, and beyond that of traditional privacy protection issues. Digital watermarking and 3D printed products present a future where objects can be searched for with nothing more than the equivalent of a Google search word. This presents challenges for privacy, due to the possibility of tracking the use of individually printed objects.

The empirical research carried out in this study indicates that some 3D printing companies are aware of the issues. Likewise, that Chinese, UK, EU and US governments have required consent for the use of private data which (presumably) could include 3D printed products shows a concern about the use of information that can identify individuals. However, 3D printing and digital watermarking specifically has not been considered by any Government or regulatory body, nor has there been any regulatory research carried out on the matter. This is surprising, because the unique ability developed to search physical objects can reveal an incredible amount of information about the day-to-day activities of individual people, having the potential to undermine much of the protections that have been built up around privacy. Privacy principles cannot be extended carte blanche to digital watermarking within the context of 3D printing.

We therefore have proposed a set of solutions utilising the existing privacy framework, in terms of soft regulation and international principles. We have suggested an international provision, a statement of privacy, a requirement that watermarks be identified, and self-regulation in terms of protecting individual privacy. It is imperative that there is an attempt to protect the individual privacy of users with regard to digital watermarking, as failure to do so will erode the applicability of concepts such as privacy in the digital age. Our proposals help to ensure the protection of individual privacy in an increasingly digitised world.

BIBLIOGRAPHY:

African Union Commission Personal Data Protection Guidelines for Africa, Jun. 27, 2014.

American Convention on Human Rights, Article 11, Nov. 21, 1969, 1144 U.N.T.S. 123

Anderson, C., Makers: The New Industrial Revolution (Random House Business Books, 2012).

Anon, Creative Commons, Creative Commons (Jul. 12, 2019) at https://creativecommons.org/

Anon, How does bitcoin work? , bitcoin.org (Jul.12, 2019) at https://bitcoin.org/en/faq#how-does-bitcoin-work .

Anon, Information Technology -- Automatic Identification and Data Capture Techniques -- QR Code bar code symbology specification ISO 18004 , International Organization For Standardization (Jul. 12, 2019) at https://www.iso.org/standard/62021.html

Anon, Information technology -- Automatic identification https://www.iso.org/home.html

Anon, Introduction , China Internet Network Information Center(Jul. 12, 2019)at https://cnnic.com.cn/ScientificResearch/LeadingEdge/fymly1/ .

Anon, Purchase Your ISBNs Online , Nielson UK ISBN Agency (Jul. 12, 2019)at http://www.isbn.nielsenbook.co.uk/controller.php?page=121 .

Anon, QR Code.com , qrcode.com (Jul. 12, 2019)at http://www.qrcode.com/en/index.html .

Anon, The Copyright Hub, Copyright Hub (Jul. 12, 2019) at www.copyrighthub.org ; Anon, National Copyright Administration of the People's Republic of China, National Copyright Administration Of The People's Republic Of China (Jul. 12, 2019) at http://www.ncac.gov.cn/

Anon, The DOI system , DOI.ORG (Jul. 12, 2019) at https://www.doi.org/ .

Anon, Treaties and Contracting Parties: Contracting Parties > WIPO Copyright Treaty > China , World Intellectual Property Organization(Jul. 12, 2019)at http://www.wipo.int/treaties/en/remarks.jsp?cnty_id=1989C .

Anon, WIPO Arbitration and Mediation Center, World Intellectual Property Organization (Jul. 12, 2019) at 1, at http://www.wipo.int/edocs/pubdocs/en/arbitration/919/wipo_pub_919.pdf (no publication details available).

Anon, WIPO-Administered Treaties: Contracting Parties > WIPO Copyright Treaty (Total Contracting Parties : 96) , World Intellectual Property Organization(Jul. 12, 2019)at http://www.wipo.int/treaties/en/ShowResults.jsp?treaty_id=16

Arab Charter on Human Rights, Article 1, Jun. 27, 1981, 999 U.N.T.S. 302.

BBC, Controversial copyright law rejected by EU parliament BBC NEWS (Jul. 12, 2019) at https://www.bbc.co.uk/news/technology-44712475 .

Benedict, EPFL unveils 3D printed miniature microfluidic device for monitoring critical blood levels , 3DERS(Jul. 12, 2019)at http://www.3ders.org/articles/20151026-epfl-unveils-3d-printed-microfluidic-device-for-monitoring-critical-blood-levels.html .

Berne Convention for the Protection of Literary and Artistic Works, Sept. 9, 1886, as revised in Paris on July 24, 1971 and amended in 1979, S. Treaty Doc. No. 99-27 (1986) [The 1979 amended version does not appear in UNTS or ILM, but the 1971 Paris revision is available at 1161 UNTS 30 (1971)].

Bowker, Get your book discovered, ISBN.org (Jul. 12, 2019) http://www.isbn.org/ .

Burns, M., The STL Format Standard Data Format for Fabbers , fabbers.com (Aug. 12, 2018, 11.00AM) at http://www.fabbers.com/tech/STL_Format .

Chan, H., Choo, H., Osuji, O., & Griffin, J., Intellectual Property Rights and Emerging Technology: 3d Printing in China (Routledge, 2018).

Cole, D., "Assessing the Leakers: Criminals or Heroes?" (2015) 8 Journal of National Security Law and Policy 107

COM/2016/0593 final, Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market.

Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies, U.N. Doc. HRI/GEN/1/Rev.6 at 142 (2003).

Convention on the Protection of All Migrant Workers and Members of their Families, Article 14, Dec. 18, 1990, 2220 U.N.T.S. 3

Convention on the Rights of Persons with Disabilities, Article 22, Dec. 13, 2006, 2518 U.N.T.S. 283

Convention on the Rights of the Child, Article 16, Nov. 20, 1989, 1588 U.N.T.S. 3

Copyright Law of the PRC (中华人民共和国著作权法) and the Implementing Rules for the Copyright Law of the PRC (著作权法实施条例)

Council of Europe Protocol to update the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981, 1496 UNTS 66.

Crawford, K., & Schultz, J., Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms , 55 Boston College Law Review 93 (2014)

Digital Millennium Copyright Act, 17 U.S.C. §§ 1201-1202 (1998)

Directive 2001/29 of the European Parliament and of the Council of 22 May 2001 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society, 2001 O.J. (L. 167); in the UK, that Directive is implemented by s.296ZA-ZG CDPA 1988 via the implementing regulations (The Copyright and Related Rights Regulations 2003, SI 2003/2498).

Dreyfus, N., France - The Hadopi Law, Two Years After 13 E-Commerce Law And Policy 8 (2011).

European Convention on Human Rights, Article 8, Nov. 11, 1950, 213 U.N.T.S. 222

Gooch, R., DRM: Copy Protection vs. Consumer Frustration , MUSICTANK (Aug. 12, 2018, 19.54PM)" http://www.musictank.co.uk/product/drm-copy-protection-vs-consumer-frustration-transcript/#3eCLAg89e5CL7eAe.99 .

Grey, S., The New Spymasters' (Viking, 2015);

Griffin, J., & Nair, A., Scientia potentia est: Making threats of copyright infringement 27. International Review Of Law, Computers, and Technology 1 (2013).

Griffin, J., The Digital Economy Act 2010 and the impact on semiotic certainty 24 International Review Of Law, Computers, and Technology 251 (2010).

Gubbia, J,. et al Internet of Things (IoT): A vision, architectural elements, and future directions 29 Future Generation Computer Systems 1645 (2013)

HIGGS, E., The Information State In England (Palgrave, 2004).

H.R.C Res. 34/7, "The Right to Privacy in the Digital Age", H.R.C. 34thSess, U.N. Doc. A/HRC/RES/34/7, (Apr. 7, 2017).

Human Rights Committee General Comment No. 16, Article 17 (Right to Privacy): The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation (Twenty-third session, 1988).

Human Rights Council Res. 28/16, The Right to Privacy in the Digital Age, Resolution of the Human Rights Council, 28th Sess., A/HRC/RES/28/16, 4(a) (1 Apr. 2015).

International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171.

Investigatory Powers Act UK 2016, c.25 ('Snoopers Charter').

Jeremy Thomas, Research 3D print living blood vessels , Lawrence Livermore National Laboratory (Aug. 12, 2018, 14.16PM) at https://www.llnl.gov/news/researchers-3d-print-living-blood-vessels

Joyce, D., Privacy in the Digital Era: Human Rights Online? 16 Melbourne Journal Of International Law 1 (2015)

Kim, Q., What happens when House of Cards goes live? Marketplace, at https://www.marketplace.org/2015/02/27/business/what-happens-netflix-when-house-cards-goes-live .

Kossof, P.,First Draft Revision of Chinese Copyright Law Under XI Administration Demonstrates Commitment to Significant Copyright Reform, Asia Law Portal (2014); https://www.lexology.com/library/detail.aspx?g=5c6d2dd5-6598-462b-859b-065ee5c38157

Li, P., 3D Bioprinting Technologies: Patents, Innovation and Access, 6 Law, Innovation And Technology 282 (2014)

Li, P., et al., Intellectual Property and 3D Printing: A Case Study on 3D Chocolate Printing 9 JIPL&P 322 (2014)

Marrakesh Agreement Establishing the World Trade Organization, Apr. 15, 1994, 1867 U.N.T.S. 154, 33 I.L.M. 1144 (1994).

Menon, S., Policy Initiative Dilemmas Surrounding Media Convergence: A Cross National Perspective 24 Prometheus 59 (2007).

Milanovic, M., Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age 56(1) Harvard International Law Journal 81 (2015)

Mingde, L., The Process of Intellectual Property Law Reform in China, 8 Queen Mary Journal Of Intellectual Property 26 (2018).

Munns, C., & Basu, S., Privacy and Healthcare Data, (Ashgate, 2016).

Newman, J., Oculus Rift privacy policy prompts lawmaker concern , PC WORLD(Jul. 12, 2019)at http://www.pcworld.com/article/3053903/virtual-reality/oculus-rift-privacy-policy-prompts-lawmaker-concern.html .

NSA PRISM Powerpoint Slides (Jul. 12, 2019)at https://archive.org/details/NSA-PRISM-Slides ; The Guardian, The NSA Files, THE GUARDIAN (Aug. 12 2018 14.50PM) at https://www.theguardian.com/us-news/the-nsa-files

Polonetsky, J., & Tene, O., Privacy And Big Data: Making Ends Meet 66 Stan. L. Rev. 25 (2013)

Polonetsky, J., & Tene, O., Privacy in the Age of Big Data 64 Stan. L. Rev. Online 63 (2012).

Polonetsky, J., & Tene, O., Big Data for All: Privacy and User Control in the Age of Analytics , 11 Northwestern Journal Of Technology And Intellectual Property 239 (2013)

Porup, J., The Internet of Things is a Surveillance Nightmare, Daily Dot (Mar. 20 2016), 00.01 AM),

Raviv, D., Explainer: what is 4d printing? , The Conversation(Jul. 12, 2019)at http://theconversation.com/explainer-what-is-4d-printing-35696 .

Rayburn, C., After Napster , 6 Va. J.L. & Tech. 16 (2001

Reese, A, Will merging access controls and rights controls undermine the structure of anti-circumvention law? , 18 Berkeley Technology Law Journal 619 (2003).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJL 119.

Report of the Special Rapporteur on the Right to Privacy, H.R.C. 31st Sess, U.N. Doc. A/HRC/31/64, (Nov. 24, 2016).

Report of the Special Rapporteur on the Right to Privacy, U.N.G.A 73rd Sess, U.N. Doc. A/73/45712, (Oct. 17 2018).

Report of the Special Rapporteur on the Right to Privacy, H.R.C. 37th Sess, U.N. Doc. A/HRC/37/62, (Oct. 25, 2018).

Report of the Special Rapporteur on the Right to Privacy, H.R.C. 40th Sess, U.N. Doc. A/HRC/40/63, (Feb. 27, 2019).

Report of the U.N. High Commissioner for Human Rights, The Right to Privacy in the Digital Age , H.R.C. 27th Sess, U.N. Doc. A/HRC/27/37 (June 30, 2014).

Report of the U.N. High Commissioner for Human Rights, The Right to Privacy in the Digital Age , H.R.C. 39th Sess, U.N. Doc. A/HRC/39/29, (Aug. 3, 2018).

Richards, N., & King, J., Three Paradoxes of Big Data , 66 Stanford Law Review Online 41 (2013)

Romero-Moreno, F., & Griffin, J., Criminal Copyright Proposals: Are They Appropriate in the Information Era? 7 European Journal Of Law And Technology 2 (2016)

Rubinstein, I., Big Data: The End of Privacy or a New Beginning? , 3 International Data Privacy Law 74 (2013)

Savelyev, A., Copyright in the blockchain era: promises and challenges 34 Computer Law And Security Review 550 (2018).

Singer, P., & Friedman, A., Cybersecurity And Cyberwar (OUP, 2014)

T.R.I.P.S., Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, 1869 U.N.T.S. 299, 33 I.L.M. 1197, Art 13 (1994).

Townsend, M., Snooper's charter: Most Britons unaware of Tory plans, survey finds, The Guardian(Jul. 12, 2019)at https://www.theguardian.com/technology/2016/jun/05/snoopers-charter-most-britons-unaware-tory-plans ;

U.N.G.A. Res. 68/167, "The Right to Privacy in a Digital Age", U.N. GAOR, 68th Sess., U.N. Doc. A/RES/68/167 (Jan. 21, 2014).

U.N.G.A. Res. 73/179, "The Right to Privacy in the Digital Age", U.N.G.A. 73rd Sess, U.N. Doc. A/RES/73/179, (Jan. 21, 2019).

Universal Declaration of Human Rights, Article 12, G. A. Res. 217 (III) A, U.N. Doc. A/RES/217(III) (Dec. 10, 1948).

Van Der Berg, B., Van Der Hof, S., Kosta, E., 3d Printing: Legal, Ethical And Economic Dimensions (Springer, 2016)

Vincent, D., Privacy: A Short History (Polity Press, 2016),

Vinton Cerf et al, Specification of Internet Transmission Control Program, IETF (Aug. 12, 2018, 15.00PM) at http://www.ietf.org/rfc/rfc0675.txt .

W.I.P.O. Copyright Treaty,Art 12,Dec 20, 1996, 36 I.L.M. 65 (1997)

W.I.P.O. Performances and Phonograms Treaty, Art 19, Dec. 12, 1996, 36 I.L.M. 76 (1997).

Wang, S., & Hunt, K., Chinese company implants 3-D printed blood vessels into monkeys CNN (Jul. 12, 2019) at https://edition.cnn.com/2017/01/10/health/china-3d-printed-blood-vessels/index.html

Zhegu, M., Handbook Of Research On Digital Transformations 19 (Edward Elgar, 2016).

* Assistant Professor, School of Law, University of Durham.

** Associate Professor, School of Law, University of Exeter.

[1] The empirical data was gathered as part of AHRC, Newton Fund and Ningbo Science and Technology Bureau project '3D printing in China' AH/N504300/1. The interviews were undertaken with representatives of 3D printing companies spread across different regions of China. The companies were working with different materials (including plastics and metals) within various areas of the 3D printing market, including the production of hardware and software. The interviewees were selected through opportunity sampling: 3D printing companies operating in key locations were contacted with details of the research project and interviews were set up with representatives of companies willing and able to be interviewed. The interviews lasted for 45 minutes to one hour. They were semi-structured, so as to allow the interviews to be tailored to the concerns and interests of the interviewees, but followed a common interview protocol. The interviewees were informed of their ability to withdraw from the study and indicated their preference regarding the anonymity of their interview data. The data was processed and held in accordance with the ethical guidelines of the lead University. Edited anonymised transcripts of the interviews can be found in Chan, Choo, Griffin and Osuji (eds), Intellectual Property Rights and Emerging Technology: 3D printing in China (Routledge, 2018).

[2] See the mandate of the Special Rapporteur on the Right to Privacy, outlined in Human Rights Council Res. 28/16, The Right to Privacy in the Digital Age, Resolution of the Human Rights Council, 28th Sess., A/HRC/RES/28/16, 4(a) (1 Apr. 2015).

[3] Jayavardhana Gubbia, et al Internet of Things (IoT): A vision, architectural elements, and future directions 29 FUTURE GENERATION COMPUTER SYSTEMS 1645 (2013); JM Porup, The Internet of Things is a Surveillance Nightmare DAILY DOT (Jul. 12, 2019), http://kernelmag.dailydot.com/issue%C2%ADsections/staff

%C2%ADeditorials/16196/internet%C2%ADof%C2%ADthings%C2%ADsurveillance%C2%ADnightmare/ ;.

[4] Serenetie Wang & Katie Hunt, Chinese company implants 3-D printed blood vessels into monkeys CNN (Jul. 12, 2019) at https://edition.cnn.com/2017/01/10/health/china-3d-printed-blood-vessels/index.html . Watermarking can be applied to the vessel so that e.g. infra red scans could detect alterations in pressure and shape.

[5] Jeremy Thomas, Research 3D print living blood vessels , LAWRENCE LIVERMORE NATIONAL LABORATORY (Jul. 12, 2019) at https://www.llnl.gov/news/researchers-3d-print-living-blood-vessels ; Benedict, EPFL unveils 3D printed miniature microfluidic device for monitoring critical blood levels , 3DERS (Jul. 12, 2019) at http://www.3ders.org/articles/20151026-epfl-unveils-3d-printed-microfluidic-device-for-monitoring-critical-blood-levels.html .

[6] Dan Raviv, Explainer: what is 4d printing? , THE CONVERSATION (Jul. 12, 2019) at http://theconversation.com/explainer-what-is-4d-printing-35696 .

[7] Oculus Rift, for example, tracks user's eyes and stores that data thus enabling the company to know how long each user looks as a particular object. See inter alia Jard Newman, Oculus Rift privacy policy prompts lawmaker concern , PC WORLD (Jul. 12, 2019) at http://www.pcworld.com/article/3053903/virtual-reality/oculus-rift-privacy-policy-prompts-lawmaker-concern.html .

[8] S Menon, Policy Initiative Dilemmas Surrounding Media Convergence: A Cross National Perspective 24 PROMETHEUS 59 (2007).

[9] See inter alia CHRIS ANDERSON, MAKERS: THE NEW INDUSTRIAL REVOLUTION (Random House Business Books, 2012), BIBI VAN DER BERG, SIMONE VAN DER HOF, ELENI KOSTA, 3D PRINTING: LEGAL, ETHICAL AND ECONOMIC DIMENSIONS (Springer, 2016), Phoebe Li, 3D Bioprinting Technologies: Patents, Innovation and Access, 6 LAW, INNOVATION AND TECHNOLOGY 282 (2014); P Li, et al., Intellectual Property and 3D Printing: A Case Study on 3D Chocolate Printing 9 JIPL&P 322 (2014), HING KAI CHAN et al, INTELLECTUAL PROPERTY AND EMERGING TECHNOLOGY: 3D PRINTING IN CHINA supra 1.

[10] For details seeBowker, Get your book discovered , ISBN.ORG (Jul. 12, 2019) http://www.isbn.org/ .

[11] See http://www.qrcode.com/en/index.html .

[12] PETER SINGER AND ALLAN FRIEDMAN, CYBERSECURITY AND CYBERWAR (OUP, 2014); STEPHEN GREY, THE NEW SPYMASTERS' (Viking, 2015); Consider for example the US NSA slides -National Security Agency, NSA PRISM Powerpoint Slides (Jul. 12, 2019) at https://archive.org/details/NSA-PRISM-Slides ; The Guardian, The NSA Files, THE GUARDIAN (Jul. 12, 2019) at https://www.theguardian.com/us-news/the-nsa-files ; Mark Townsend, Snooper's charter: Most Britons unaware of Tory plans, survey finds, THE GUARDIAN (Jul. 12, 2019)

at https://www.theguardian.com/technology/2016/jun/05/snoopers-charter-most-britons-unaware-tory-plans ; UK Investigatory Powers Act UK 2016, c.25 ('Snoopers Charter')

[13] Queena Kim, What happens when House of Cards goes live? MARKETPLACE, at https://www.marketplace.org/2015/02/27/business/what-happens-netflix-when-house-cards-goes-live .

[14] This is one of the principles behind Web 2.0.

[15] See inter alia DAVID VINCENT, PRIVACY: A SHORT HISTORY (Polity Press, 2016), EDWARD HIGGS, THE INFORMATION STATE IN ENGLAND (Palgrave, 2004).

[16] Cartoon by Peter Steiner, THE NEW YORKER, 5 July, 1993.

[17] Glenn Fleischman, Everybody Knows You're a Dog, BOINGBOING (Jul. 12, 2019) at https://boingboing.net/2013/10/17/everybody-knows-youre-a-do.html .

[18] Vinton Cerf et al, Specification of Internet Transmission Control Program, IETF (Jul. 12, 2019) at http://www.ietf.org/rfc/rfc0675.txt .

[19] Anon, Introduction , CHINA INTERNET NETWORK INFORMATION CENTER (Jul. 12, 2019) at https://cnnic.com.cn/ScientificResearch/LeadingEdge/fymly1/ .

[20] See inter alia Anon, Purchase Your ISBNs Online , NIELSON UK ISBN AGENCY (Jul. 12, 2019) at http://www.isbn.nielsenbook.co.uk/controller.php?page=121 .

[21] Anon, Information Technology -- Automatic Identification and Data Capture Techniques -- QR Code bar code symbology specification ISO 18004 , INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (Jul. 12, 2019) at https://www.iso.org/standard/62021.html ; Anon, QR Code.com , QRCODE.COM (Jul. 12, 2019) at http://www.qrcode.com/en/index.html .

[22] Anon, The DOI system , DOI.ORG (Jul. 12, 2019) at https://www.doi.org/ .

[23] Admin, What's the Alternative for Sharing STL Files , PDF3D (Jul. 12, 2019) at https://www.pdf3d.com/whats-the-alternative-for-sharing-stl-files/ .

[24] Marshall Burns, The STL Format Standard Data Format for Fabbers , FABBERS.COM (Jul. 12, 2019) at http://www.fabbers.com/tech/STL_Format .

[25] National Security Agency, NSA PRISM Powerpoint Slides, supra 12. For detail on these revelations, see, for example, D. Cole, "Assessing the Leakers: Criminals or Heroes?" (2015) 8 Journal of National Security Law and Policy 107.

[26] Ibid .

[27] Kate Crawford and Jason Schultz, Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms , 55 BOSTON COLLEGE LAW REVIEW 93 (2014); Jules Polonetsky & Omer Tene, Privacy And Big Data: Making Ends Meet 66 STAN. L. REV. 25 (2013); Neil Richards and Jonathan King, Three Paradoxes of Big Data , 66 STANFORD LAW REVIEW ONLINE 41 (2013); Ira Rubinstein, Big Data: The End of Privacy or a New Beginning? , 3

INTERNATIONAL DATA PRIVACY LAW 74 (2013); Jules Polonetsky and Omer Tene, Big Data for All: Privacy and User Control in the Age of Analytics , 11 NORTHWESTERN JOURNAL OF TECHNOLOGY AND INTELLECTUAL PROPERTY 239 (2013), Jules Polonetsky and Omer Tene, Privacy in the Age of Big Data 64 STAN. L. REV. ONLINE 63 (2012).

[28] Interview 10.

[29] Article 12:

"Obligations concerning Rights Management Information

(1) Contracting Parties shall provide adequate and effective legal remedies against any person knowingly performing any of the following acts knowing, or with respect to civil remedies having reasonable grounds to know, that it will induce, enable, facilitate or conceal an infringement of any right covered by this Treaty or the Berne Convention:

(i) to remove or alter any electronic rights management information without authority;

(ii) to distribute, import for distribution, broadcast or communicate to the public, without authority, works or copies of works knowing that electronic rights management information has been removed or altered without authority.

(2) As used in this Article, "rights management information" means information which identifies the work, the author of the work, the owner of any right in the work, or information about the terms and conditions of use of the work, and any numbers or codes that represent such information, when any of these items of information is attached to a copy of a work or appears in connection with the communication of a work to the public".

[30] Digital Millennium Copyright Act, 17 U.S.C. §§ 1201-1202 (1998) ;Directive 2001/29 of the European Parliament and of the Council of 22 May 2001 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society, 2001 O.J. (L. 167); in the UK, that Directive is implemented by s.296ZA-ZG CDPA 1988 via the implementing regulations (The Copyright and Related Rights Regulations 2003, SI 2003/2498).

[31] Anon, WIPO-Administered Treaties: Contracting Parties > WIPO Copyright Treaty (Total Contracting Parties : 96) , WORLD INTELLECTUAL PROPERTY ORGANIZATION (Jul. 12, 2019) at http://www.wipo.int/treaties/en/ShowResults.jsp?treaty_id=16 Note Macau & Hong Kong- Anon, Treaties and Contracting Parties: Contracting Parties > WIPO Copyright Treaty > China , WORLD INTELLECTUAL PROPERTY ORGANIZATION (Jul. 12, 2019) at http://www.wipo.int/treaties/en/remarks.jsp?cnty_id=1989C .

[32] If so, balancing is broadly based around freedom of expression and right to privacy - key ECHR cases then cited by UK courts are Von Hannover v Germany [2004] EMLR 21, Von Hannover v Germany (no. 2) [2012] EMLR 16 and Von Hannover v Germany (No. 3) - Reference Application No.8772/10. Examples of differing implementation of No 1 are in Murray v Express Newspapers and Big Pictures [2007] EWHC 1980 (Ch) and [2008] EWCA Civ 446. Further discussion is in Campbell v MGN [2004] 2 AC 457 and inter alia Douglas v Hello No 1 [2001] EMLR 199 and Douglas v Hello No3/No6 [2005] EWCA Civ 595.

[33] Coco v Clark [1969] RPC 41.

[34] Ibid.,, but note the desire of Megarry VC, who gave the Coco judgment, that it should be flexible - Thomas Marshall (exports) v Guinle [1979] 1 Ch 227.

[35] Vidal-Hall v Google Inc.[2015] FSR 25.

[36] Ibid., at 751.

[37] Norwich Pharmacal Co. & Others v Customs and Excise Commissioners [1974] AC 133

[38] Golden Eye (International) Ltd v Telefónica UK Ltd [2013] R.P.C. 18.

[39] Ibid,. at 454-455.

[40] C-275/06 Productores de Música de España (Promusicae) v Telefónica de España SAU ECR 2008 I-00271.

[41] Ibid., para 71.

[42] Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (Sup. Ct.).

[43] Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 518 F.Supp.2d 1197 (C.D.Cal. 2007).

[44] A & M Records, Inc. v. Napster, Inc., 284 F.3d 1091 (9th Cir. 2002) at 1233.

[45] A & M Records, Inc. v. Napster, Inc., 284 F.3d 1091 (9th Cir. 2002) at 1098.

[46] Corey Rayburn, After Napster , 6 VA. J.L. & TECH. 16 (2001) at §22."In Octo ber 13, however, SDMI director Leonardo Chiariglione said that Salon.com's report of the hacked watermarks was "completely wrong, unfounded, anonymous slander."Still, Salon.com's source said all four SDMI technologies were broken and that SDMI was trying to cover up their failure to develop secure watermarks." Citing Janelle Brown, Cracked or Not? The SDMI Sage Continues: Did hackers successfully break watermarks designed to protect digital music? SALOM.COM (Oct. 19, 2000) at www.salom.com.

[47] A & M Records, Inc. v. Napster, Inc., 284 F.3d 1091 (9th Cir. 2002) at 1097.

[48] It could be argued that this is due to the context of the case, since it was not concerned with the revealing of a specific user identity but the conduct of Napster. Privacy has to date been protected through the John Doe case law, and in any event concerns the revealing of information about potential piracy rather than day to day use of data.

[49] C-360/10 Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV [2012] 2 CMLR 18; C-70/10 Scarlet Extended SA v SABAM [2012] ECDR 4.

[50] COM/2016/0593 final, Proposal for a Directive Of The European Parliament and of the Council on copyright in the Digital Single Market.

[51] Article 13, ibid . It should be noted that the UK has made clear that this Directive will not be implemented as a result of Brexit - see Anon, Article 13: UK will not implement EU copyright law available at https://www.bbc.co.uk/news/technology-51240785 (last accessed 10th March 2020).

[52] Article 17 Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC., OJ/L 130/92.

[53] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJL 119.In short, there is the right to be informed, of access to collected data, to rectification, erasure, to restrict processing, and there are rights to data portability, to object and rights in relation to automated decision making and profiling.

[54] Article 6 GDPR lists, as the bases for lawfulness of processing: "a. the data subject has given consent to the processing of his or her personal data for one or more specific purposes; b. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps a the request of the data subject prior to entering into a contract; c. processing is necessary for compliance with a legal obligation to which the controller is subject; d. processing is necessary in order to protect the vital interests of the data subject or of another natural person; e. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; f. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child".

[55] Article 4 Ibid . Under Article 4,"'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"

[56] 中华人民共和国网络安全法(PRC Cyberspace Law) 2017.

[57] Ibid., Article 37.

[58] Universal Declaration of Human Rights, Article 12, G. A. Res. 217 (III) A, U.N. Doc. A/RES/217(III) (Dec. 10, 1948); Convention on the Rights of the Child, Article 16, Nov. 20, 1989, 1588 U.N.T.S. 3; Convention on the Protection of All Migrant Workers and Members of their Families, Article 14, Dec. 18, 1990, 2220 U.N.T.S. 3; Convention on the Rights of Persons with Disabilities, Article 22, Dec. 13, 2006, 2518 U.N.T.S. 283; European Convention on Human Rights, Article 8, Nov. 11, 1950, 213 U.N.T.S. 222; American Convention on Human Rights, Article 11, Nov. 21, 1969, 1144 U.N.T.S. 123; Arab Charter on Human Rights, Article 1, Jun. 27, 1981, 999 U.N.T.S. 302. For further international and regional instruments, see: http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/Internationalstandards.aspx

[59] Other regional measures include the Council of Europe Protocol to update the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28,

1981, 1496 UNTS 66, and the African Union Commission Personal Data Protection Guidelines for Africa, Jun. 27, 2014.

[60] Universal Declaration of Human Rights, ibid ,Article 12 ("no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks").

[61] International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171.

[62] Human Rights Committee General Comment No. 16, Article 17 (Right to Privacy): The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation (Twenty-third session, 1988), Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies, U.N. Doc. HRI/GEN/1/Rev.6 at 142 (2003). See DanielJoyce, Privacy in the Digital Era: Human Rights Online? 16 MELBOURNE JOURNAL OF INTERNATIONAL LAW 1 (2015)for discussion of the application of General Comment No 16 to issues raised by the development of new technology.

[63] U.N.G.A. Res. 68/167, "The Right to Privacy in a Digital Age", U.N. GAOR, 68thSess., U.N. Doc. A/RES/68/167 (Jan. 21, 2014).

[64] Marko Milanovic, Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age 56(1) HARVARD INTERNATIONAL LAW JOURNAL 81 (2015), at 85-6.

[65] U.N.G.A., supra 54 , para. 5.

[66] U.N. High Commissioner for Human Rights, The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights , U.N. Doc. A/HRC/27/37 (June 30, 2014).

[67] Ibid , paras 1-4.

[68] Ibid , para 18.

[69] U.N. High Commissioner for Human Rights, The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights , U.N. Doc. A/HRC/27/37 (June 30, 2014).para 19-20.

[70] Ibid .

[71] Ibid .

[72] Ibid .

[73] Ibid.

[74] As noted by Joyce, much of G.A. Res. 69/166 repeats G.A. Res. 68/167, but it does provide "recognition of the role of business and its responsibilities".DanielJoyce, Privacy in the Digital Era: Human Rights Online? 16 MELBOURNE JOURNAL OF INTERNATIONAL LAW 1, 9 (2015).

[75] Report of the Special Rapporteur on the Right to Privacy, H.R.C. 31st Sess, U.N. Doc. A/HRC/31/64, para. 7 (Nov. 24, 2016).

[76] Ibid , para. 8.

[77] Ibid , para. 8.

[78] Ibid , paras. 45-55.

[79] Ibid , para. 50.

[80] Ibid , para. 55.

[81] Report of the Special Rapporteur on the Right to Privacy, H.R.C. 37th Sess, U.N. Doc. A/HRC/37/62, (Oct. 25, 2018). Report of the Special Rapporteur on the Right to Privacy, U.N.G.A 73rd Sess, U.N. Doc. A/73/45712, (Oct. 17 2018). Report of the Special Rapporteur on the Right to Privacy, H.R.C. 40th Sess, U.N. Doc. A/HRC/40/63, (Feb. 27, 2019).

[82] Report of the U.N. High Commissioner for Human Rights, The Right to Privacy in the Digital Age, H.R.C. 39th Sess, U.N. Doc. A/HRC/39/29, (Aug. 3, 2018).

[83] H.R.C Res. 34/7, "The Right to Privacy in the Digital Age", H.R.C. 34th Sess, U.N. Doc. A/HRC/RES/34/7, (Apr. 7, 2017).

[84] U.N.G.A. Res. 73/179, "The Right to Privacy in the Digital Age", U.N.G.A. 73rd Sess, U.N. Doc. A/RES/73/179, (Jan. 21, 2019).

[85] Interviews 5 and 7 and 22.

[86] Interviews 5, 10 and 11.

[87] Interview 13: "For those like the lamp, we will not care too much. But for the product of medical use, we have interest to follow up as it is related to people's life".

[88] Interview 5: "As a service provider, the ability of trace is not so important. However, for academic and product development, it is quite important".

[89] Interview 18.

[90] Interview 5 and 15.

[91] Interview 18 and 7.

[92] Interview 5.

[93] Interview 5.

[94] Interview 5.

[95] Interview 18.

[96] One interviewee questioned the value of tracking technology for the company. See Interview 10.

[97] Interviews 14 and 18: "I think for type two or second class medical devices, it may be some need to use the technology you mentioned, because they want to know exactly where the material come from, or what kind of material it is".

[98] Interview 15.

[99] Interviews 10 and 12.

[100] Interview 10: "In terms of tracking violation of IP, which involves business secrets. The procedure of negotiation and lawsuit could be tedious because regulations vary across countries, and Chinese legislation is pretty weak regarding protection of IP. So we try not to focus on tracking, instead, we can upgrade the product to protect the business. In fact it is a general situation of Chinese IP owners that updating and upgrading are more practical".

[101] Interview 11.

[102] Interview 11.

[103] Interview 18.

[104] Interview 15.

[105] Interview 8: "The code is, for the time being, kept in a separate file from the scan but that they were trying to collate the two".

[106] Interview 21.

[107] Some that said that they were not using tracking at the moment indicated that they were considering it. See Interview 17.

[108] Interview 10.

[109] Interview 16.

[110] Interview 14.

[111] Interview 7.

[112] Interview 9: "I cannot track. I gave the buyer the source code. They would do some modifications based my product. If they change the source code a little bit, it will be a new thing. They can apply for a new patent for the new thing. Therefore, it is illegal to trace that".

[113] Interview 10.

[114] Interview 17.

[115] Interview 18.

[116] Interview 18: "For example we can have sort of contact, we can translate patients name to some other code without any meaning. Then we sue the code as patents name. So in the later process we can just see the code and how their surgery goes. I think for academic research that could be okay. And we want to put on the platform; I think there will be some mechanics to protect the data from hack".

[117] Interview 18: "In the future maybe we will put it on the cloud. So the surgeon can change the surgery technic, but we have high standard of protecting patient's privacy. We will make sure their information is not leaks".

[118] Interview 5: "Never and ever. Because these things belong to the customer. Before the product is launched in the market, we shouldn't do this. Otherwise it will harm not only the markets of our customers, but also ourselves".

[119] Interview 5.

[120] Interview 11: "For us there are benefits for sure. But it's difficult to realize it because it needs market acceptance".

[121] Interview 17.

[122] Interview 17.

[123] The Special Rapporteur has noted that "consumers world-wide are increasingly aware of risks to their privacy and... will increasingly choose privacy-friendly products and services over ones which are privacy-neutral or privacy-unfriendly". See Report of the Special Rapporteur on the Right to Privacy, A/HRC/31/64, supra 72,para 50.

[124] Ibid , para 59.

[125] "If there is a market for privacy, market forces will provide for it. The rapid increase in the availability of encrypted devices and software services is a strong indicator that consumers worldwide are increasingly aware of the risks to their privacy and that they will increasingly choose privacy-friendly products and services over ones that are privacy neutral or privacy unfriendly". See ibid , para 59.

[126] It should be noted that this data was collected before the adoption of the new regulation.

[127] Interview 21.

[128] Interview 18.

[129] Interview 22.

[130] See Neil Richards and Jonathan King, Big Data and the Future in MAJILNDA ZHEGU, HANDBOOK OF RESEARCH ON DIGITAL TRANSFORMATIONS 19 (Elgar, 2016).

[131] Interview 18: "...when comes to medical area, I think the standard will be just higher then platform right now. We are very serious about it, and in the future, the government will have high standard too. So we will try our best to meet the government".

[132] Interview 18.

[133] Interview 22.

[134] This supports the assertion that international developments can fill gaps in domestic practice. SeeNeil Richards and Jonathan King, Big Data and the Future supra 130at 17-18: " even where domestic law is silent, the global nature of the information economy means that actors within the US will increasingly fall within the regulatory authority of foreign data protection

authorities. Early examples of this phenomenon include the attempts by French courts to hold Yahoo! Liable for the sale of Nazi memorabilia... More recently, the Court of justice for the European Union held that Google was required to delete search results for a Spanish man who had been adjudged bankrupt in the past... Although judgments of these sorts rarely have extraterritorial application as a matter of law, they tend to have extraterritorial application as a matter of effect".

[135] Interviews 1 and 2.

[136] Golden Eye (International) Ltd v Telefónica UK Ltd [2013] R.P.C. 18.

[137] Felipe Romero-Moreno & James Griffin, Criminal Copyright Proposals: Are They Appropriate in the Information Era? 7 EUROPEAN JOURNAL OF LAW AND TECHNOLOGY 2 (2016)

[138] James Griffin, THE DIGITAL ECONOMY ACT 2010 AND THE IMPACT ON SEMIOTIC CERTAINTY 24 INTERNATIONAL REVIEW OF LAW, COMPUTERS AND TECHNOLOGY 251 (2010).

[139] Neil Dreyfus, France - The Hadopi Law, Two Years After 13 E-COMMERCE LAW AND POLICY 8 (2011).

[140] Note that we have not suggested to use the word "consent" in the proposals, since this concept is problematic in this context just as it is with the current crop of data protection laws, due to the fact that even a basic watermark could be used in a manner to invade individual privacy.

[141] TRIPS: Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299, 33 I.L.M. 1197, Art 13 (1994); Note also Art 9(2) Berne Convention for the Protection of Literary and Artistic Works, Sept. 9, 1886, as revised in Paris on July 24, 1971 and amended in 1979, S. Treaty Doc. No. 99-27 (1986) [The 1979 amended version does not appear in UNTS or ILM, but the 1971 Paris revision is available at 1161 UNTS 30 (1971)].

[142] Further backed up by the inclusion of CMI provisions inWIPO Copyright Treaty,Art 12,Dec 20, 1996, 36 I.L.M. 65 (1997); WIPO Performances and Phonograms Treaty, Art 19, Dec. 12, 1996, 36 I.L.M. 76 (1997).

[143] Annex 2 of the Marrakesh Agreement Establishing the World Trade Organization, Apr. 15, 1994, 1867 U.N.T.S. 154, 33 I.L.M. 1144 (1994).

[144] See e.g. von Hannover - Von Hannover v Germany [2004] EMLR 21, Von Hannover v Germany (no. 2) [2012] EMLR 16 and Von Hannover v Germany (No. 3) - Reference Application No.8772/10 supra32

[145] Copyright Law of the PRC (中华人民共和国著作权法) and the Implementing Rules for the Copyright Law of the PRC (著作权法实施条例); Paul Kossof, First Draft Revision of Chinese Copyright Law Under XI Administration Demonstrates Commitment to Significant Copyright

Reform, Asia Law Portal (2014); https://www.lexology.com/library/detail.aspx?g=5c6d2dd5-6598-462b-859b-065ee5c38157

[146] See Li Mingde, The Process of Intellectual Property Law Reform in China,

8 QUEEN MARY JOURNAL OF INTELLECTUAL PROPERTY 26 (2018).

[147] See above, infra section 3.1.

[148] See Section 4.3.

[149] Anon, Creative Commons, CREATIVE COMMONS (Aug. 12, 2018, 20.00PM) at https://creativecommons.org/

[150] Note - "In 2002, the International Federation of the Phonographic Industry (IFPI) developed voluntary guidelines for its members on the

labelling of CDs containing DRMs, but the IFPI guidelines do not appear to have had much influence on industry practice" - Richard Gooch, DRM: Copy Protection vs. Consumer Frustration , MUSICTANK (Aug. 12, 2018, 19.54PM)" http://www.musictank.co.uk/product/drm-copy-protection-vs-consumer-frustration-transcript/#3eCLAg89e5CL7eAe.99 .

[151] This has arguably occurred with DRM mechanisms - see Anthony Reese, Will merging access controls and rights controls undermine the structure of anti-circumvention law? , 18 BERKELEY TECHNOLOGY LAW JOURNAL 619 (2003).

[152] The application of this would build upon existing knowledge rules, e.g. as found in the UK in ZYX Music v King [1997] 2 All ER 129.

[153] See supra Section 4.3.

[154] Similar to the bitcoin system - Anon, How does bitcoin work? , BITCOIN.ORG (Aug.12, 2018, 03.44AM) at https://bitcoin.org/en/faq#how-does-bitcoin-work .

[155] See Section 4.3.

[156] Alexander Savelyev, Copyright in the blockchain era: promises and challenges 34 COMPUTER LAW AND SECURITY REVIEW 550 (2018).

[157] It is worth nothing that in the Snowden files, it is apparent that sufficiently strong protection has yet to be broken by Governments, let alone individuals, due to the amount of computing power required - s upra 12.

[158] Anon, Information technology -- Automatic identification https://www.iso.org/home.html supra 21for an example of an ISO standard for QR codes.

[159] Anon, How does bitcoin work? , supra 154.

[160] Interview 17.

[161] Anon, The Copyright Hub, COPYRIGHT HUB (Aug.12, 2018, 04.04AM) at www.copyrighthub.org ; Anon, National Copyright Administration of the People's Republic of China, NATIONAL COPYRIGHT ADMINISTRATION OF THE PEOPLE'S REPUBLIC OF CHINA (Aug.12, 2018, 05.32AM) at http://www.ncac.gov.cn/

[162] https://ico.org.uk/

[163] As originally permitted under s55(c)(1) Data Protection Act 1998.

[164] See Christina Munns & Subhajit Basu, Privacy and Healthcare Data, (Ashgate, 2016). The reader may wish to look at the example of the Public Benefit and Privacy Panel for Health and Social Care in Scotland, see https://www.informationgovernance.scot.nhs.uk/pbpphsc/ .

[165] See Anon, WIPO Arbitration and Mediation Center, WORLD INTELLECTUAL PROPERTY ORGANIZATION (Aug.12, 2018, 09.08PM) at 1, at http://www.wipo.int/edocs/pubdocs/en/arbitration/919/wipo_pub_919.pdf (no publication details available).

[166] Ibid , at 1-6.

[167] Infra section 4.2 and 5.2.3.

[168] Interview 19.

[169] Interview 19.

[170] Interview 17.

[171] It is worth recalling that there are no unjustified threats provisions for copyright law. See James Griffin & Abhilash Nair, Scientia potentia est: Making threats of copyright infringement 27. INTERNATIONAL REVIEW OF COMPUTERS, LAW AND TECHNOLOGY 1 (2013).